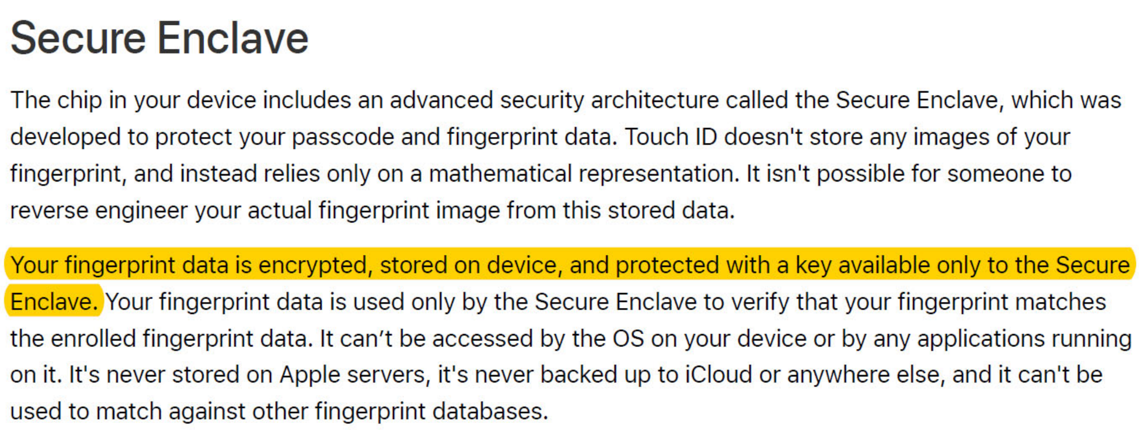
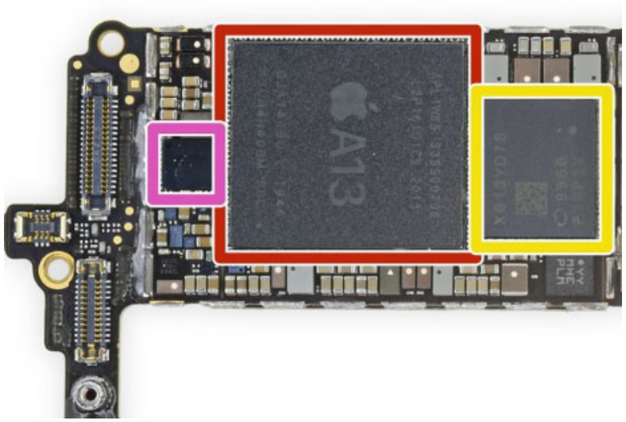
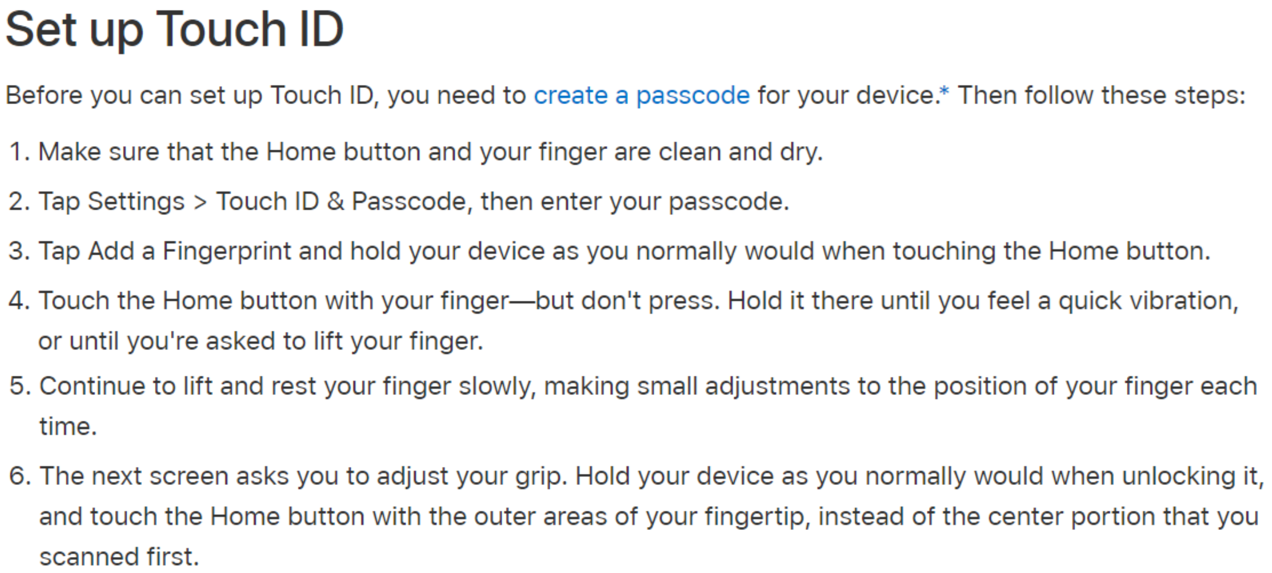
EXHIBIT I

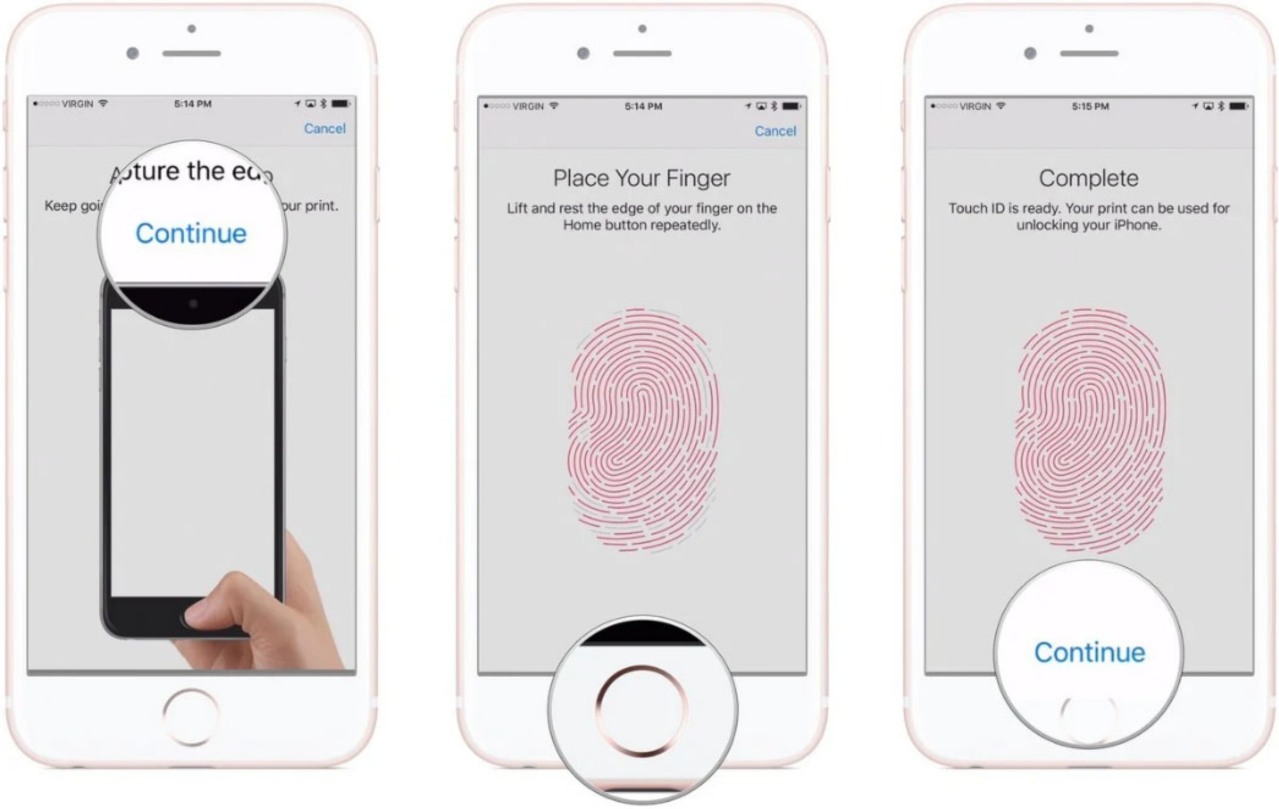
Claim Chart for U.S. Patent No. 9,665,705 ("the '705 Patent")

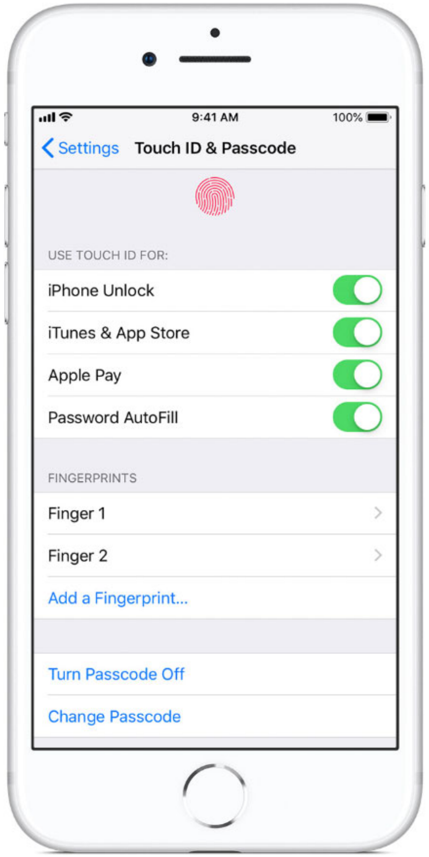
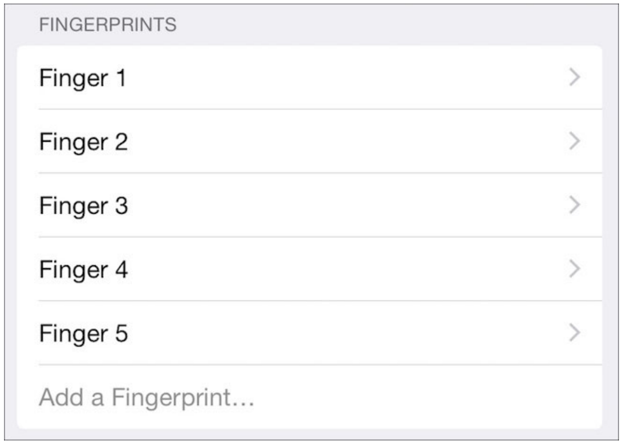
The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone type cellular phones and Apple iPad type tablets, including the Apple iPhone SE (2nd generation) and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '705 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '705 Patent literally and, to the extent not literally, under the doctrine of equivalents.

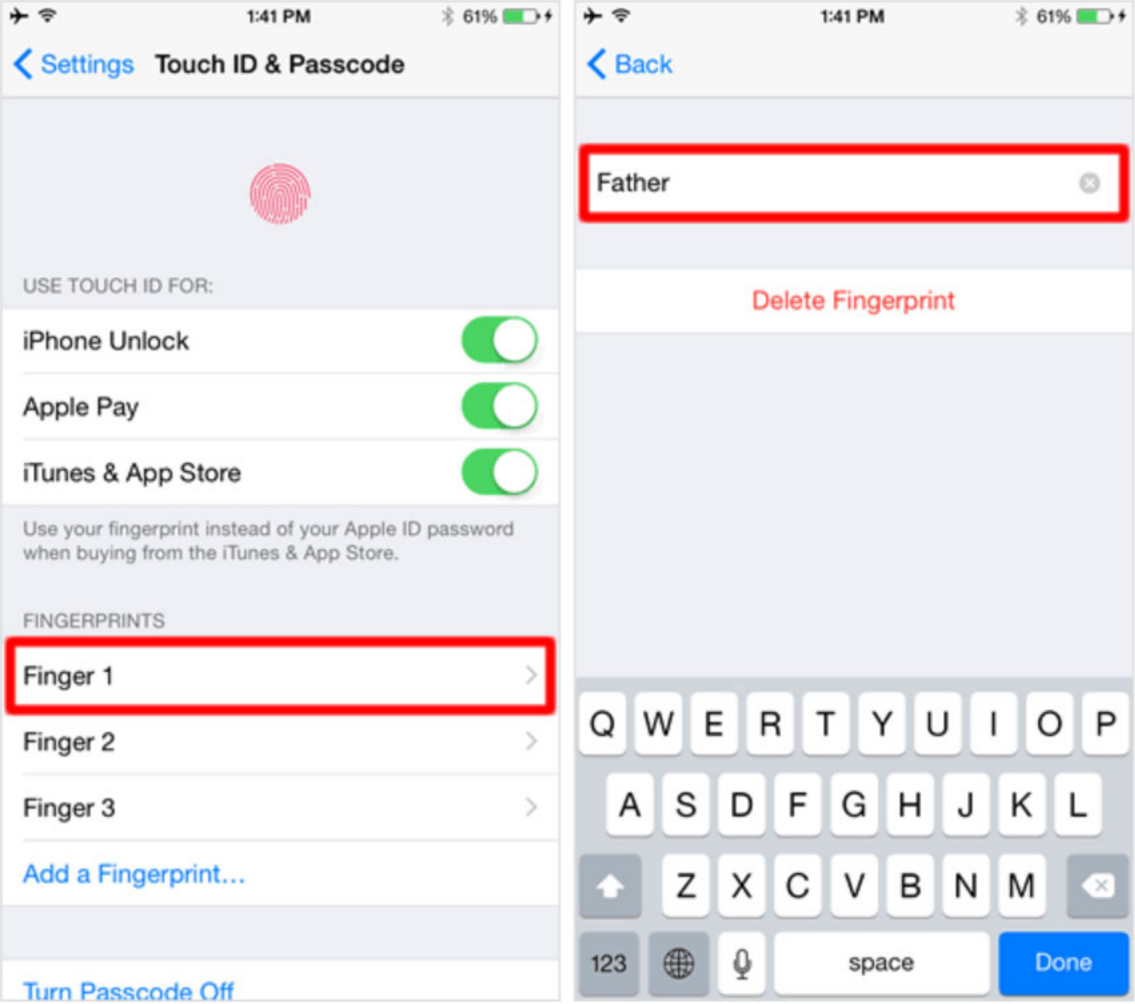
Claim 1	**Apple iPhone SE (2nd generation)**
1. A system for providing secure access to a controlled item, the system comprising:	To the extent that the preamble is deemed to be a limitation, the Apple iPhone SE is configured to use a system in accordance with this claim.
1a. a memory comprising a database of biometric signatures;	**The Apple iPhone SE includes a memory comprising a database of encrypted fingerprint data.** More specifically, the Apple iPhone SE has a secure enclave in the A13 chip that stores a database of an encrypted mathematical representation of fingerprints used for Touch ID.  Secure Enclave The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data. Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587

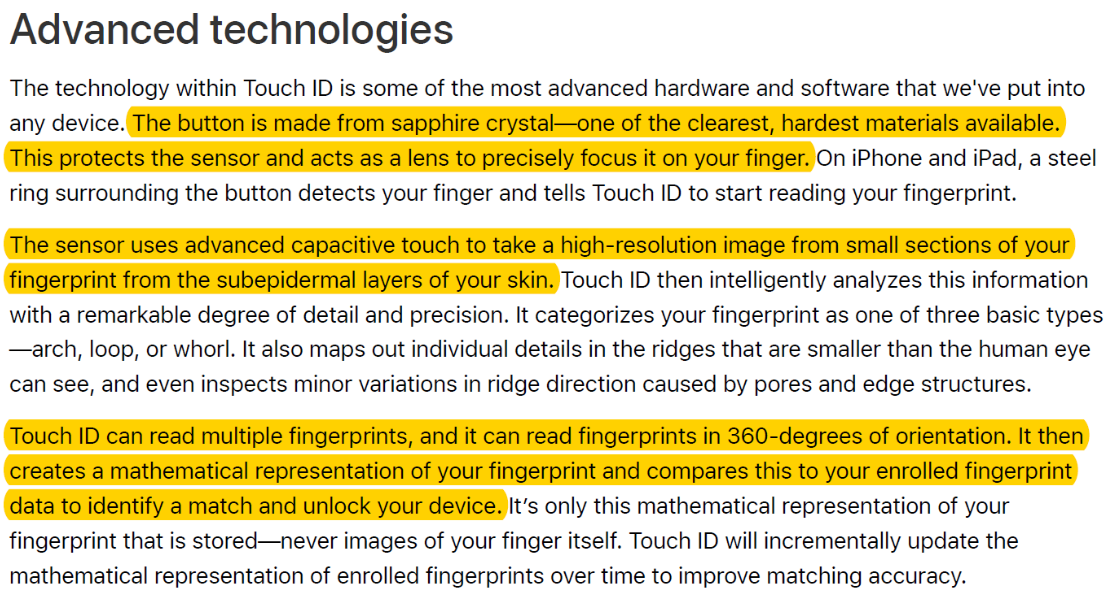
Claim 1	**Apple iPhone SE (2nd generation)**
	 ● Apple APL1W85 A13 Bionic SoC layered over Samsung K3UH4H40BM-SGCL (presumably 3 GB LPDDR4X) https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

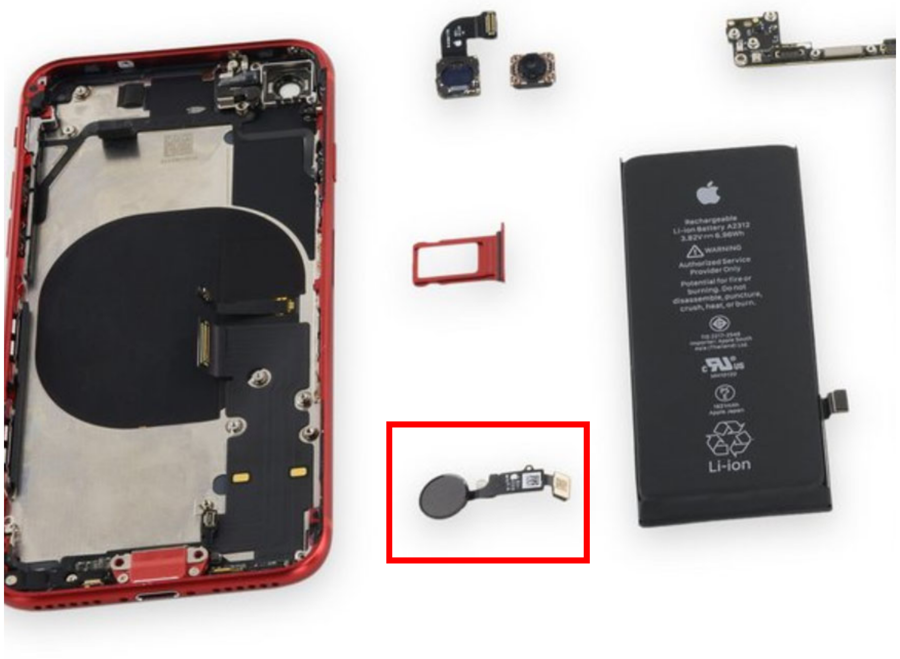
Claim 1	**Apple iPhone SE (2nd generation)**
	 **Set up Touch ID** Before you can set up Touch ID, you need to create a passcode for your device.* Then follow these steps: 1. Make sure that the Home button and your finger are clean and dry. 2. Tap Settings > Touch ID & Passcode, then enter your passcode. 3. Tap Add a Fingerprint and hold your device as you normally would when touching the Home button. 4. Touch the Home button with your finger—but don't press. Hold it there until you feel a quick vibration, or until you're asked to lift your finger. 5. Continue to lift and rest your finger slowly, making small adjustments to the position of your finger each time. 6. The next screen asks you to adjust your grip. Hold your device as you normally would when unlocking it, and touch the Home button with the outer areas of your fingertip, instead of the center portion that you scanned first. https://support.apple.com/en-us/HT201371

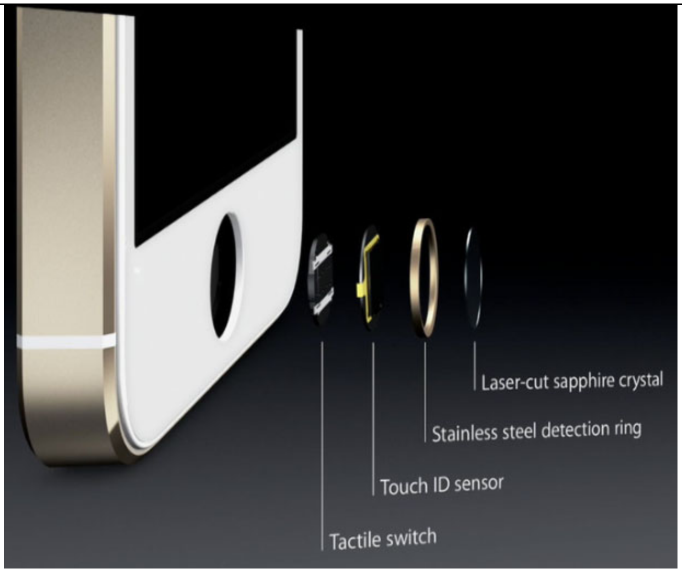
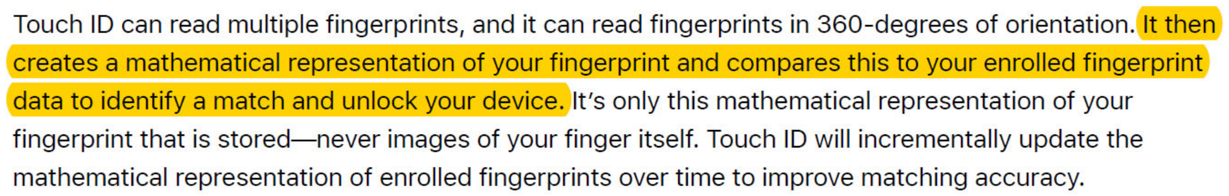
Claim 1	**Apple iPhone SE (2nd generation)**
	 VIRGIN 5:14 PM Cancel ture the ed Keep goi our print. Continue VIRGIN 5:14 PM Cancel Place Your Finger Lift and rest the edge of your finger on the Home button repeatedly. VIRGIN 5:15 PM Complete Touch ID is ready. Your print can be used for unlocking your iPhone. Continue https://www.imore.com/how-to-use-touch-id-iphone-ipad

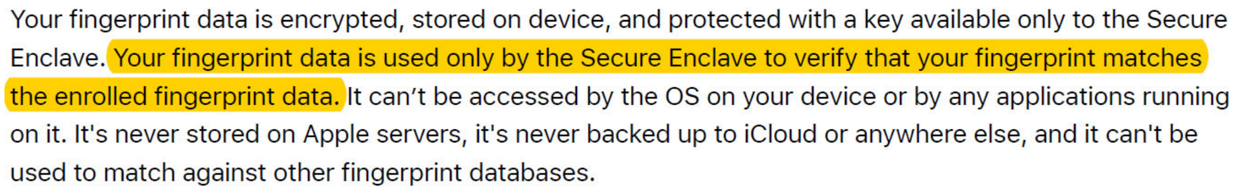
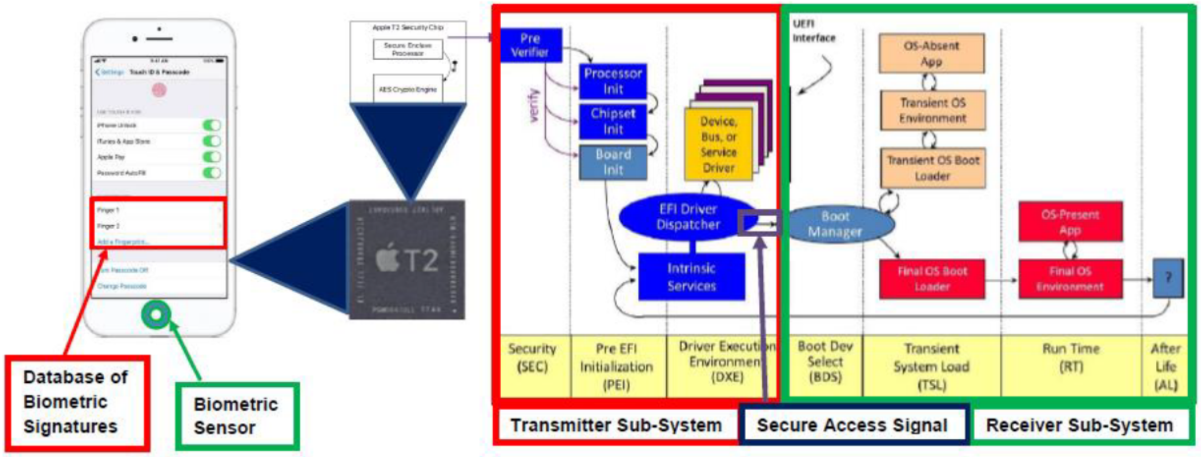
Claim 1	**Apple iPhone SE (2nd generation)**
	Additionally, the Apple iPhone SE allows users to add multiple fingerprints and label each fingerprint whatever they prefer. It makes it easier to recognize different fingerprints when users share their device with other family members or friends.  9:41 AM 100% Settings Touch ID & Passcode USE TOUCH ID FOR: iPhone Unlock iTunes & App Store Apple Pay Password AutoFill FINGERPRINTS Finger 1 Finger 2 Add a Fingerprint... Turn Passcode Off Change Passcode  FINGERPRINTS Finger 1 Finger 2 Finger 3 Finger 4 Finger 5 Add a Fingerprint... https://www.howtogeek.com/205525/how-to-add-touch-id-fingerprints-to-iphone-or-ipad/

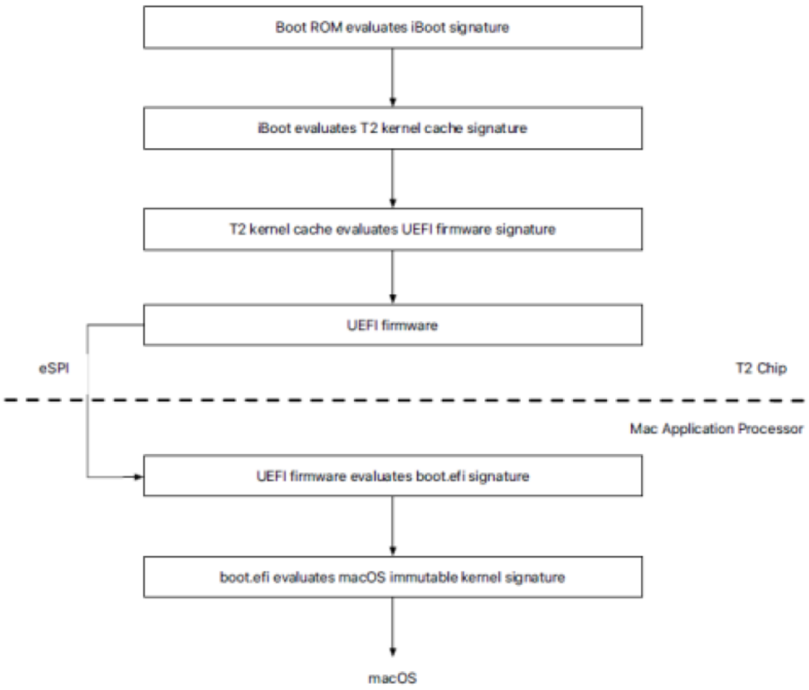
Claim 1	**Apple iPhone SE (2nd generation)**
	 1:41 PM 61% Settings Touch ID & Passcode USE TOUCH ID FOR: iPhone Unlock Apple Pay iTunes & App Store Use your fingerprint instead of your Apple ID password when buying from the iTunes & App Store. FINGERPRINTS Finger 1 Finger 2 Finger 3 Add a Fingerprint... Turn Passcode Off 1:41 PM 61% Back Father Delete Fingerprint Q W E R T Y U I O P A S D F G H J K L Z X C V B N M 123 space Done https://en.teach-me.biz/iphone/settings/touch-id.html

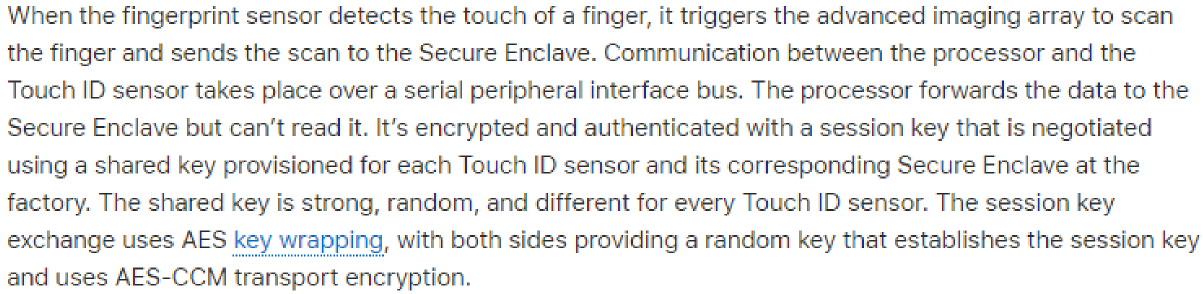
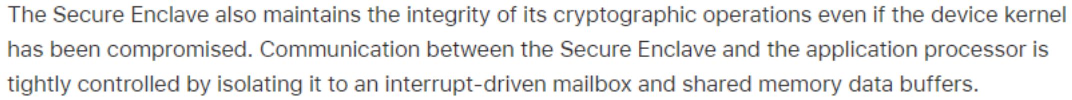
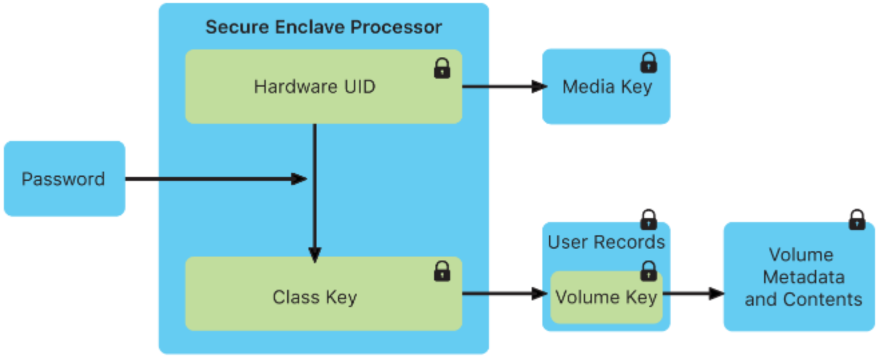
Claim 1	**Apple iPhone SE (2nd generation)**
1b. a transmitter sub-system comprising:	As set forth in elements 1b1, 1b2, and 1b3 below, the Apple iPhone SE includes a transmitter subsystem.
1b1. a biometric sensor configured to receive a biometric signal;	**The Apple iPhone SE includes a biometric sensor configured to receive a biometric signal.** More specifically, the Apple iPhone SE has a home button that includes a sensor to detect fingerprints and activates a Touch ID to start reading the user's fingerprint.  Advanced technologies The technology within Touch ID is some of the most advanced hardware and software that we've put into any device. The button is made from sapphire crystal—one of the clearest, hardest materials available. This protects the sensor and acts as a lens to precisely focus it on your finger. On iPhone and iPad, a steel ring surrounding the button detects your finger and tells Touch ID to start reading your fingerprint. The sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types —arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy. https://support.apple.com/en-us/HT204587

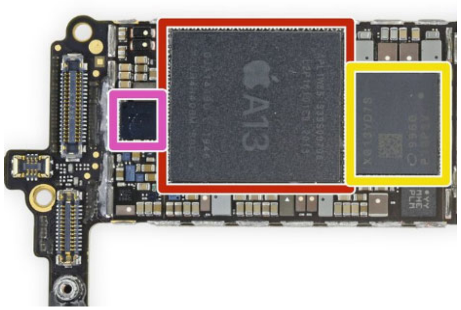
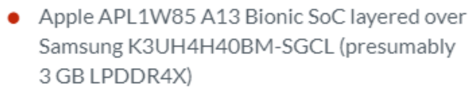
Claim 1	**Apple iPhone SE (2nd generation)**
	 https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

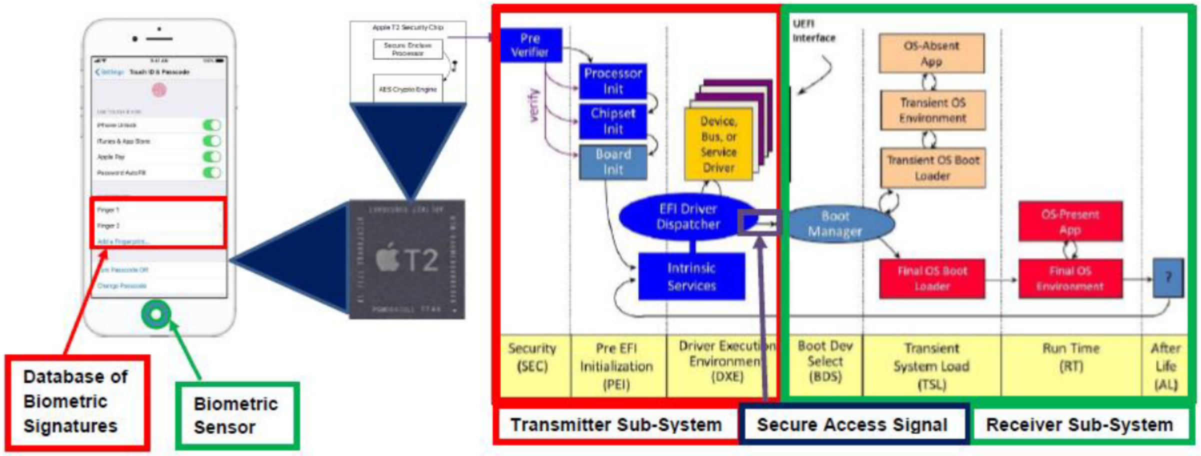
Claim 1	**Apple iPhone SE (2nd generation)**
	 Laser-cut sapphire crystal Stainless steel detection ring Touch ID sensor Tactile switch https://www.imore.com/how-touch-id-works
1b2. a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and	**The Apple iPhone SE includes a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.** More specifically, the Apple iPhone SE has a secure enclave processor (SEP) that matches fingerprints against the registered fingerprint data.  Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy.

Claim 1	**Apple iPhone SE (2nd generation)**
	 Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases. https://support.apple.com/en-us/HT204587 Secure Enclave is a coprocessor of Apple's T2 Security Chip. *Apple T2 Security Chip Security Overview* (Oct. 2018) at 3. Apple's Secure Enclave is a separate processor built into the device's main system. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/.
1b3. a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and	**The Apple iPhone SE includes a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.** More specifically, the iPhone SE includes a secure enclave processor (SEP) that includes a transmitter block and sends a secure access signal based on the fingerprints data received from the sensor.  Database of Biometric Signatures Biometric Sensor Apple T2 Security Chip Secure Enclave Processor AES Crypto Engine T2 Pre Verifier verify Processor Init Chipset Init Board Init Device, Bus, or Service Driver EFI Driver Dispatcher Intrinsic Services UEFI Interface OS-Absent App Transient OS Environment Transient OS Boot Loader Boot Manager OS-Present App Final OS Boot Loader Final OS Environment ? Security (SEC) Pre EFI Initialization (PEI) Driver Execution Environment (DXE) Boot Dev Select (BDS) Transient System Load (TSL) Run Time (RT) After Life (AL) Transmitter Sub-System Secure Access Signal Receiver Sub-System

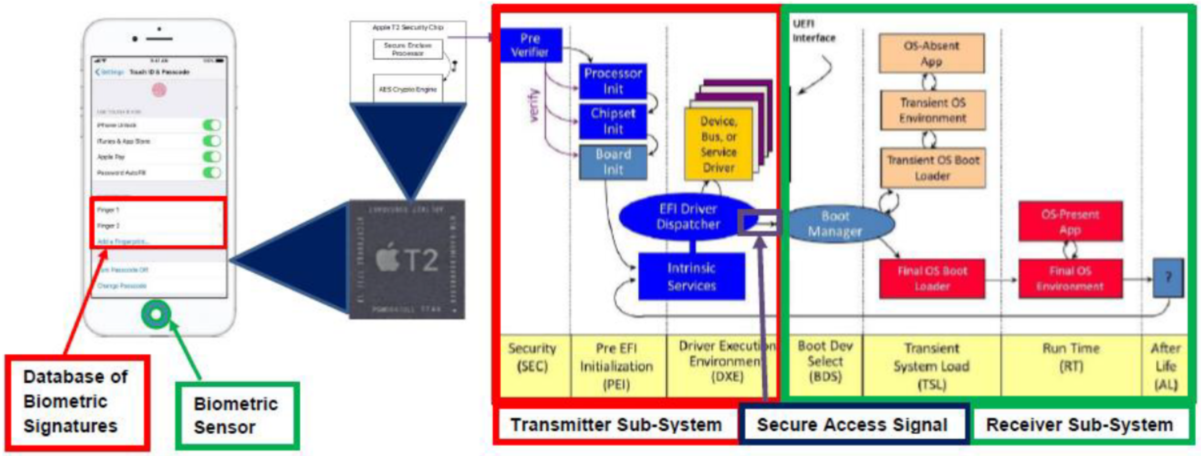
Claim 1	**Apple iPhone SE (2nd generation)**
	As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green). In the figure below, the transmission is from the T2 Chip to the Mac Application Processor via the Enhanced Serial Peripheral Interface ("eSPI") bus:  Boot ROM evaluates iBoot signature iBoot evaluates T2 kernel cache signature T2 kernel cache evaluates UEFI firmware signature UEFI firmware eSPI T2 Chip Mac Application Processor UEFI firmware evaluates boot.efi signature boot.efi evaluates macOS immutable kernel signature macOS *Apple T2 Security Chip Security Overview* (Oct. 2018) at 8.

Claim 1	**Apple iPhone SE (2nd generation)**
	 When the fingerprint sensor detects the touch of a finger, it triggers the advanced imaging array to scan the finger and sends the scan to the Secure Enclave. Communication between the processor and the Touch ID sensor takes place over a serial peripheral interface bus. The processor forwards the data to the Secure Enclave but can't read it. It's encrypted and authenticated with a session key that is negotiated using a shared key provisioned for each Touch ID sensor and its corresponding Secure Enclave at the factory. The shared key is strong, random, and different for every Touch ID sensor. The session key exchange uses AES key wrapping, with both sides providing a random key that establishes the session key and uses AES-CCM transport encryption. https://support.apple.com/guide/security/touch-id-security-sec0f02a0f7f/web  The Secure Enclave also maintains the integrity of its cryptographic operations even if the device kernel has been compromised. Communication between the Secure Enclave and the application processor is tightly controlled by isolating it to an interrupt-driven mailbox and shared memory data buffers.  Secure Enclave Processor Hardware UID Media Key Password Class Key User Records Volume Key Volume Metadata and Contents The Secure Enclave processor. https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web

Claim 1	**Apple iPhone SE (2nd generation)**
	  ● Apple APL1W85 A13 Bionic SoC layered over Samsung K3UH4H40BM-SGCL (presumably 3 GB LPDDR4X) https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

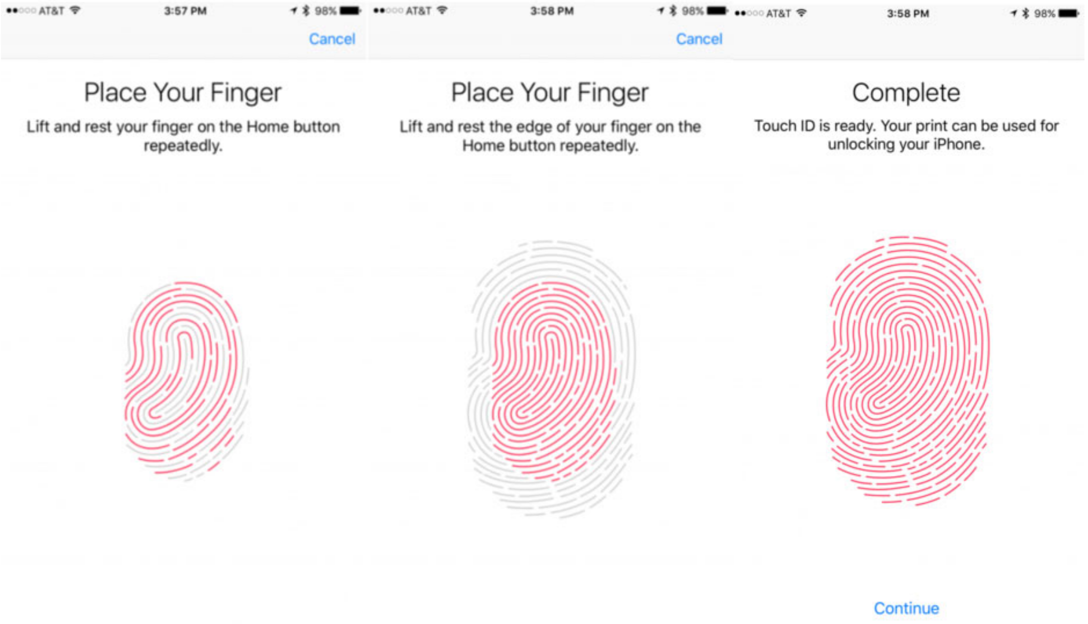
<u>**Claim 1**</u>	<u>**Apple iPhone SE (2nd generation)**</u>
1c. a receiver sub-system comprising:	As set forth in elements 1c1 and 1c2 below, the Apple iPhone SE includes a receiver sub-system.
1c1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and	**The Apple iPhone SE includes receiver sub-system configured to receive the transmitted secure access signal.** More specifically, the iPhone SE includes an application processor (AP) that receives encrypted secure biometric data from a secure enclave processor (SEP).  Touch ID & Passcode iPhone Unlock iTunes & App Store Apple Pay Password AutoFill Finger 1 Finger 2 Add a Fingerprint... Turn Passcode Off Change Passcode Database of Biometric Signatures Biometric Sensor Apple T2 Security Chip Secure Enclave Processor AES Crypto Engine T2 Pre Verifier verify Processor Init Chipset Init Board Init Device, Bus, or Service Driver EFI Driver Dispatcher Intrinsic Services UEFI Interface Boot Manager OS-Absent App Transient OS Environment Transient OS Boot Loader Final OS Boot Loader OS-Present App Final OS Environment ? Security (SEC) Pre EFI Initialization (PEI) Driver Execution Environment (DXE) Boot Dev Select (BDS) Transient System Load (TSL) Run Time (RT) After Life (AL) Transmitter Sub-System Secure Access Signal Receiver Sub-System As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green).
1c2. provide conditional access to the controlled item dependent upon said information;	**The Apple iPhone SE includes receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.** More specifically, the iPhone SE includes an application processor (AP) that can grant access to the device based on the matching fingerprints data received from a secure enclave processor (SEP).

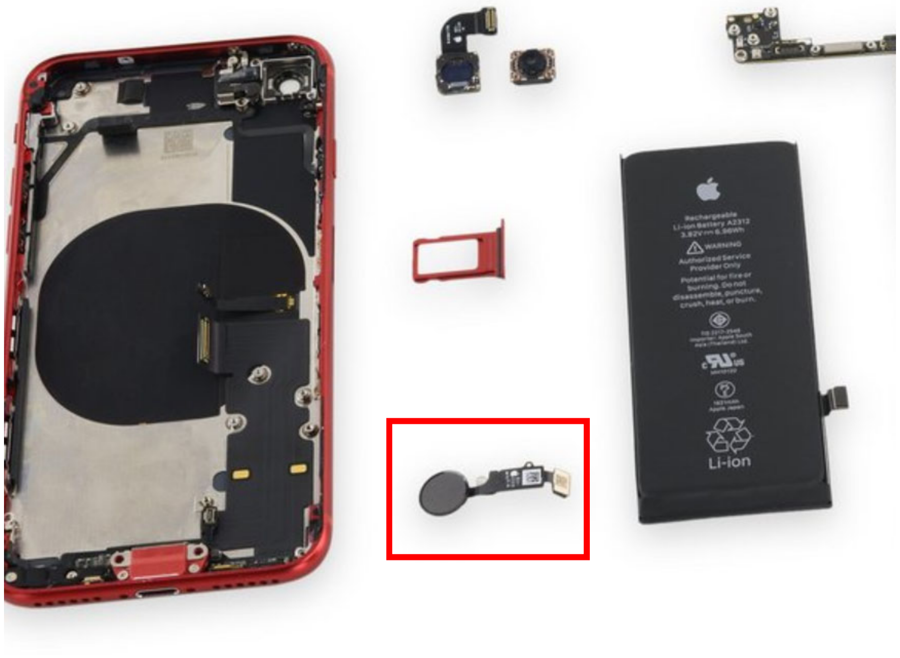
<table>
<tr><th><u>Claim 1</u></th><th><u>Apple iPhone SE (2nd generation)</u></th></tr>
<tr><td></td><td>

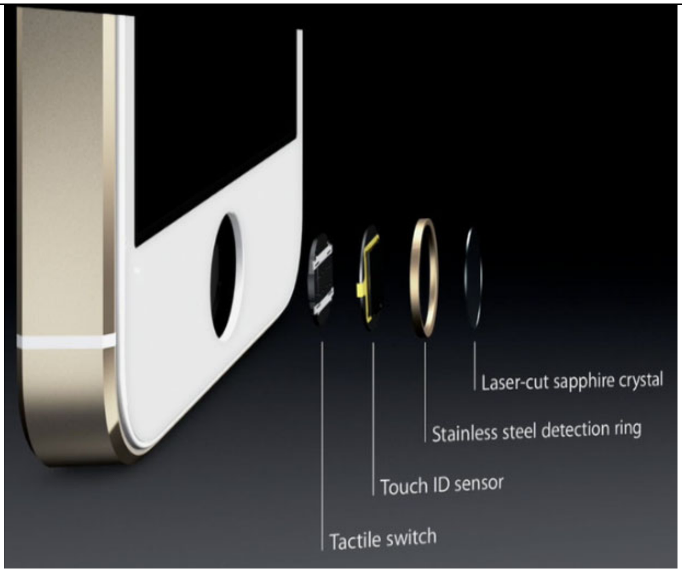


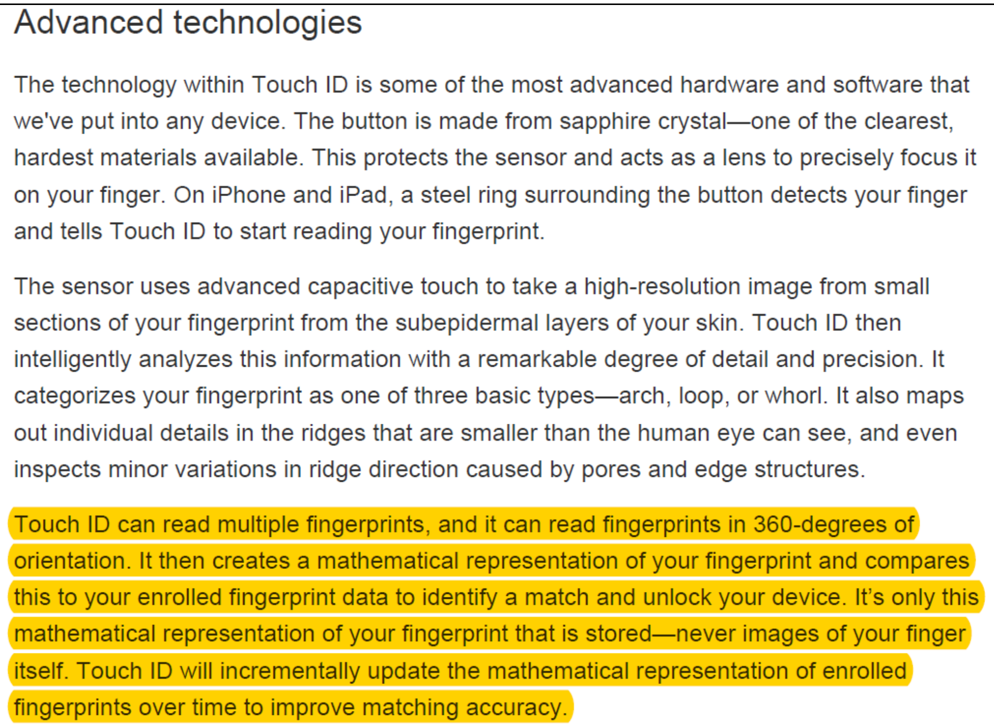
As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green).

</td></tr>
</table>

Claim 1	**Apple iPhone SE (2nd generation)**
1d. wherein the transmitter sub-system controller is further configured to:	The Apple iPhone SE includes a transmitter sub-system controller that is configured to be used as set forth in elements 1d1, 1d2, and 1d3 below.
1d1. receive a series of entries of the biometric signal, said series being characterized [characterized] according to at least one of the number of said entries and a duration of each said entry;	**The Apple iPhone SE includes transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.** More specifically, the Apple iPhone SE receives a series of fingerprint signal through a sensor by having users to touch a home button repeatedly to set up a Touch ID.  ●●○○○ AT&T 3:57 PM 98% Cancel ●●○○○ AT&T 3:58 PM 98% Cancel ●●○○○ AT&T 3:58 PM 98% Continue Place Your Finger Lift and rest your finger on the Home button repeatedly. Place Your Finger Lift and rest the edge of your finger on the Home button repeatedly. Complete Touch ID is ready. Your print can be used for unlocking your iPhone. https://www.idownloadblog.com/2016/01/14/touch-id-not-working-try-this/

Claim 1	**Apple iPhone SE (2nd generation)**
	 https://www.ifixit.com/Teardown/iPhone+SE+2020+Teardown/133066

Claim 1	**Apple iPhone SE (2nd generation)**
	 Laser-cut sapphire crystal Stainless steel detection ring Touch ID sensor Tactile switch https://www.imore.com/how-touch-id-works
1d2. map said series into an instruction; and	**The Apple iPhone SE includes transmitter sub-system controller configured to map said series into an instruction.** More specifically, the Apple iPhone SE includes a secure enclave processor (SEP) that can map a series of fingerprint signal into an instruction for encryption.

Claim 1	**Apple iPhone SE (2nd generation)**
	 Advanced technologies The technology within Touch ID is some of the most advanced hardware and software that we've put into any device. The button is made from sapphire crystal—one of the clearest, hardest materials available. This protects the sensor and acts as a lens to precisely focus it on your finger. On iPhone and iPad, a steel ring surrounding the button detects your finger and tells Touch ID to start reading your fingerprint. The sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures. Touch ID can read multiple fingerprints, and it can read fingerprints in 360-degrees of orientation. It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device. It's only this mathematical representation of your fingerprint that is stored—never images of your finger itself. Touch ID will incrementally update the mathematical representation of enrolled fingerprints over time to improve matching accuracy. https://support.apple.com/en-us/HT204587
1d3. populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an	**The Apple iPhone SE includes transmitter sub-system controller configured to populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.** More specifically, the Apple iPhone SE includes a secure enclave processor (SEP) that can generate the encrypted fingerprint data based on the instruction to determine whether the device can be unlocked.

Claim 1	**Apple iPhone SE (2nd generation)**
electronic computing device.	An Apple Touch ID device contains a database with up to five registered fingerprints. https://support.apple.com/en-us/HT201371. The controlled item is the locked operating system of the Apple device.